Agenda

1. Introduction
2. History and Background
3. Extensible Provisioning Protocol
4. Registration Data Access Protocol
5. Q & A
Registration Data Access Protocol
Registry-Registrar Functions

Internet Users

Registrar

Web

EPP

RRDS

EPP

RRDS

DNS

Registry

Data Escrow

Database

Registrant
Replacing WHOIS Protocol: Timeline

- **19 September 2011**: SSAC’s SAC 051: *The ICANN community should evaluate and adopt a replacement domain name registration data access protocol*

- **28 October 2011**: Board resolution adopts SAC 051

- **4 June 2012**: Roadmap to implement SAC 051

- **2012**: RDAP community development within IETF WG begins

- Contractual provisions in: .biz, .cat, .com, .coop, .info, .jobs, .name,
  - .org, .pro, .travel, .xxx, 2012 Registry Agreement (new gTLDs) and 2013 Registrar Accreditation Agreement

- **March 2015**: RDAP IETF RFCs published

- **26 July 2016**: RDAP Profile version 1.0 published
Why Should WHOIS (port-43) Be Replaced?

- Non-standardized format:
Why Should WHOIS (port-43) Be Replaced?

- Not internationalized:

![WHOIS Domain Information]

- Domain Information: [domain name]
  [Registrant]
  [Name Server]
  [Signing Key]
  [Contact Information: [email]]
  [Name]
  [Email]
  [Web Page]
  [Notes]
Why Should WHOIS (port-43) Be Replaced?

- Unauthenticated
  - Unable to differentiate between users

- Unable to provide differentiated service
  - The same fields are provided to all users

- Insecure
  - No support for an encrypted response

- No bootstrapping mechanism
  - No standardized way of knowing where to query

- Lack of standardized redirection/reference
  - Different workarounds implemented by TLDs
The Registration Data Access Protocol (RDAP) is a protocol designed to replace the existing WHOIS protocol and provides the following benefits:

- Standardized query, response and error messages
- Secure access to data (i.e., over HTTPS)
- Extensibility (e.g., easy to add output elements)
RDAP Features (2/2)

- Bootstrapping mechanism to easily find the authoritative server for a given query
- Standardized redirection/reference mechanism (e.g., from a registry to a registrar)
- Builds on top of the well-known web protocol, HTTP
- Internationalization support for registration data
- Optionally enables differentiated access (e.g., limited access for anonymous users, full access for authenticated users)
RDAP Examples

- Queries:
  - https://example.com/rdap/domain/blah.example.com
  - https://example.com/rdap/domains?name=example*.com
  - https://example.com/rdap/nameserver/ns1.example.co

- Responses (two pages long for one response):

```json
{
    "objectClassName" : "domain",
    "handle" : "XXXX",
    "ldhName" : "xn--fo-5ja.example",
    "unicodeName" : "foo.example",
    "variants" :
      [
        {
          "relation" : [ "registered", "conjoined" ],
          "variantNames" :
            [
              {
                "ldhName" : "xn--fo-cka.example",
                "unicodeName" : "foo.example"
              }
            ]
      ]
}
```
Internationalization

- Internationalized domain names supported in both the question and the answer

- Internationalized contact information is supported

- Contact information supports language tags in order to define the language / script of the data

- Replies are JSON formatted, which supports UTF-8

- The transport protocol is HTTP, which supports UTF-8
Bootstrapping

- In the case of new gTLDs, whois.nic.<TLD> is the standard name to find the WHOIS/web-Whois server.

- In the case of RDAP, the protocol defines standard bootstrap mechanism that allows a client to find the authoritative server for a particular <TLD>.

- RDAP specification explains how to form direct queries and basic search queries.

- [http://data.iana.org/rdap/dns.json](http://data.iana.org/rdap/dns.json)
Differentiated Access

- Differentiated access refers to the functionality of showing different subsets of RDDS fields based on who is asking (e.g., limited access for anonymous users, full access for authenticated users)

- As of today, only three gTLDs (.cat, .name, .tel) have a contract provision allowing RDDS with differentiated access

- There is a Policy Development Process (Registration Data Services PDP) in the Generic Names Supporting Organization that has differentiated access in scope
Thin Data in RDAP

- In a thin domain registry the domain contact information is held by the registrar. The registry RDDS only holds a referral to the registrar, the registration, expiry, creation, update date, name servers and domain status.

- A thick domain registry holds all of the contact information needed for the domain names.

- With RDAP, a Registry can point the end-user to the Registrar’s RDAP in order to obtain authoritative information maintained by the Registrar.
RDAP in gTLDs

RDAP RFCs:
- SHOULDs, MAYs, MUSTs
- Do not specify required elements

ICANN gTLD policies

RDDS provisions in the RA, RAA 2013, Whois advisory

gTLD RDAP Profile

Clear Requirements

gTLD RDAP Service
Transition

Present

RDDS
Web-based RDDS
WHOIS (port-43)

Short term

RDDS
Web-based RDDS
WHOIS (port-43)
RDAP

Future

RDDS
Web-based RDDS
RDAP
Engage with ICANN

Thank You and Questions
Reach us at: globalsupport@icann.org
Website: icann.org

twitter.com/icann      gplus.to/icann
facebook.com/icannorg   weibo.com/ICANNorg
linkedin.com/company/icann    flickr.com/photos/icann
youtube.com/user/icannnews   slideshare.net/icannpresentations